Wenjie Xiong

wenjie.xiong.yale@gmail.com • https://caslab.csl.yale.edu/~wenjie

Research Interest

My research interests are in hardware security, where I leverage hardware features to enhance the security of computer systems as well as identify and mitigate security vulnerabilities that are rooted in hardware designs. In particular, I have worked on new Physically Unclonable Functions (PUFs) in DRAM and its cryptographic applications. More recently, I have investigated novel covert channel attacks in processor caches, modeling and benchmarking of cache side-channel attacks.

Education

Yale University, New Haven, CT, USA **Aug. 2014 – May. 2020**

Ph.D., Electrical Engineering
M.S., Electrical Engineering *and* M.Phil., Electrical Engineering
Advisor: *Prof.* Jakub Szefer
Thesis: Hardware Security in DRAMs and Processor Caches

Peking University, Beijing, China **Sep. 2010 – Jul. 2014**

B.S., Microelectronics Thesis: Microelectrode and Circuit for Peripheral Nerve Stimulation
B.S., Psychology

Professional Experience

Facebook, MA, USA Postdoctoral Researcher **Aug. 2020– Present**

Yale Univerisity, CT, USA Postdoctoral Associate **Jun.– Jul. 2020**

Intel Labs, Hillsboro, OR, USA Security Research Intern **Jun.– Aug. 2018**

"Microarchitecture level mitigation of speculative timing side-channel attacks in cache and TLB."
Investigated existing Spectre-like attacks and analyzed each component of the attack and possible mitigation in micro-architecture. Implemented mitigation of speculative timing side-channel attacks in cache and TLB in a cycle-accurate simulator and evaluated the performance overhead.

Intel Labs, Hillsboro, OR, USA Security Research Intern **Jun.– Aug. 2017**

"Data integrity in memory with low bandwidth overhead."
Evaluated bandwidth overhead of real-world workloads in a functional simulator. Implemented algorithms in RTL and evaluated the delay and area overhead.

TU Darmstadt, Germany Graduate Researcher **Nov.– Dec. 2016**

"Rowhammer DRAM PUF."

Selected Honors and Awards

- Featured Paper in the April 2021 issue of IEEE Transactions on Computers (TC) 2021
- Honorable Mention of IEEE Micro Top Picks 2021
- Top Picks in Hardware and Embedded Security 2019
- Participant of 3rd Heidelberg Laureate Forum 2015
- Microsoft Research Graduate Women's Scholars 2015
- National Scholarship, China 2013
- Merit Student of Peking University 2012
- Wusi Scholarship of Peking University 2011
- Merit Student of Zhejiang Province 2010

Publications

Peer-reviewed Publications

1. **Wenjie Xiong**, and Jakub Szefer, "Survey of Transient Execution Attacks and their Mitigations", in ACM Computing Surveys, vol. 54, no. 3, Article 54, May 2021.

2. Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "Understanding Insecurity of Processor Caches due to Cache Timing-Based Vulnerabilities", in IEEE Security & Privacy, vol. 19, no. 3, pp. 42-49, May-June 2021.
3. Shanquan Tian, Ilias Giechaskiel, **Wenjie Xiong**, and Jakub Szefer, "Cloud FPGA Cartography using PCIe Contention", in Proceedings of the International Symposium on Field-Programmable Custom Computing Machines (FCCM), May 2021.
4. **Wenjie Xiong**, André Schaller, Nikolaos A. Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser, and Jakub Szefer, "DRAM PUFs in Commodity Devices", in IEEE Design & Test, 2021.
5. **Wenjie Xiong**, Stefan Katzenbeisser, and Jakub Szefer, "Leaking Information Through Cache LRU States in Commercial Processors and Secure Caches", in IEEE Transactions on Computers, vol. 70, no. 04, pp. 511-523, 2021. **(Featured Paper in the April 2021 issue)**
6. Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "A Benchmark Suite for Evaluating Caches' Vulnerability to Timing Attacks", in Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2020.
7. Shanquan Tian, **Wenjie Xiong**, Ilias Giechaskiel, Kasper Rasmussen, and Jakub Szefer, "Fingerprinting Cloud FPGA Infrastructures", in Proceedings of the International Symposium on Field-Programmable Gate Arrays (FPGA), 2020.
8. **Wenjie Xiong**, and Jakub Szefer, "Leaking Information Through Cache LRU States", in Proceedings of the 26th International Symposium on High-Performance Computer Architecture (HPCA), 2020. **(IEEE Micro Top Picks 2021 Honorable Mention)**
9. **Wenjie Xiong**, André Schaller, Stefan Katzenbeisser, and Jakub Szefer, "Software Protection using Dynamic PUFs", in IEEE Transactions on Information Forensics and Security (TIFS), 2019.
10. Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "Analysis of Secure Caches using a Three-Step Model for Timing-Based Attacks", in Journal of Hardware and Systems Security, 2019.
11. Shuai Chen, **Wenjie Xiong**, Yehan Xu, Bing Li, and Jakub Szefer, "Thermal Covert Channels Leveraging Package-On-Package DRAM", in Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2019.
12. Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "Secure TLBs", in Proceedings of the International Symposium on Computer Architecture (ISCA), 2019.
13. Shuwen Deng, Doğuhan Gümüşoğlu, **Wenjie Xiong**, Y. Serhan Gener, Onur Demir, and Jakub Szefer, "SecChisel Framework for Security Verification of Secure Processor Architectures", in Proceedings of the Workshop on Hardware and Architectural Support for Security and Privacy (HASP), 2019.
14. **Wenjie Xiong**, André Schaller, Stefan Katzenbeisser, and Jakub Szefer, "Dynamic Physically Unclonable Functions", in Proceedings of the Great Lakes Symposium on VLSI (GLSVLSI), 2019.
15. **Wenjie Xiong**, Nikolaos Athanasios Anagnostopoulos, André Schaller, Stefan Katzenbeisser, and Jakub Szefer, "Spying on Temperature using DRAM", in Proceedings of the Design, Automation, and Test in Europe (DATE), 2019.
16. Nikolaos Athanasios Anagnostopoulos, Tolga Arul, Yufan Fan, Christian Hatzfeld, André Schaller, **Wenjie Xiong**, Manishkumar Jain, Muhammad Umair Saleem, Jan Lotichius, Sebastian Gabmeyer, Jakub Szefer, and Stefan Katzenbeisser, "Intrinsic Run-Time Row Hammer PUFs: Leveraging the Row Hammer Effect for Run-Time Cryptography and Improved Security", in Cryptography, 2(3), p.13, 2018.
17. Shuwen Deng, **Wenjie Xiong** and Jakub Szefer, "Cache Timing Side-Channel Vulnerability Checking with Computation Tree Logic", in Proceedings of the Workshop on Hardware and Architectural Support for Security and Privacy (HASP), 2018.
18. André Schaller†, **Wenjie Xiong**†, Nikolaos Athanasios Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Boris Skoric, Stefan Katzenbeisser, and Jakub Szefer, "Decay-Based DRAM PUFs in Commodity Devices", in IEEE Transactions on Dependable and Secure Computing (TDSC), 16(3), pp.462-475, 2019. † The authors contributed equally.
19. André Schaller, **Wenjie Xiong**, Nikolaos Athanasios Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser, and Jakub Szefer, "Intrinsic Rowhammer PUFs: Leveraging the Rowhammer effect for improved security", in Proceedings of the International Symposium on Hardware Oriented Security and Trust (HOST), 2017. **(Best Student Paper Finalist)**
20. **Wenjie Xiong**, André Schaller, Nikolaos A. Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser, and Jakub Szefer, "Run-time accessible DRAM PUFs in commodity devices", in Proceedings of

the Conference on Cryptographic Hardware and Embedded Systems (CHES), 2016. **(Top Picks in Hardware and Embedded Security 2019)**

21. Huaiqiang Yu, **Wenjie Xiong**, Hongze Zhang, Wei Wang, and Zhihong Li, "A parylene self-locking cuff electrode for peripheral nerve stimulation and recording", in Journal of Microelectromechanical Systems, 23(5), pp.1025-1035, 2014.
22. Huaiqiang Yu, **Wenjie Xiong**, Hongze Zhang, Wei Wang, and Zhihong Li, "A cable-tie-type parylene cuff electrode for peripheral nerve interfaces", in IEEE 27th International Conference on Micro Electro Mechanical Systems (MEMS), 2014.
23. **Wen Jie Xiong**, Huai Qiang Yu, and Zhi Hong Li, "Design and Simulation of a Parylene-based Three-Dimensional Cuff Electrode for peripheral nerve stimulation", in Key Engineering Materials, 609, pp.1459-1463, 2014.
24. Linbo Shao, Li Wang, **Wenjie Xiong**, Xue-Feng Jiang, Qi-Fan Yang, and Yun-Feng Xiao, "Ultrahigh-Q, largely deformed microcavities coupled by a free-space laser beam", in Applied Physics Letters, 103(12), p.121102, 2013.

Technical Reports

- Shuwen Deng, Nikolay Matyunin, **Wenjie Xiong**, Stefan Katzenbeisser, Jakub Szefer, "Evaluation of Cache Attacks on Arm Processors and Secure Caches." arXiv:2106.14054
- Onur Demir, **Wenjie Xiong**, Faisal Zaghloul, and Jakub Szefer, "Survey of Approaches for Security Verification of Hardware/Software Systems", IACR Cryptology ePrint Archive 2016 (2016): 846, Sep. 2016.

News

- **Wenjie Xiong**, and Jakub Szefer, "Memristive fingerprints prove key destruction", Nature Electronics 1(10), p.527, 2018.

Patent

- Kounavis, Michael, et al. "Security-oriented compression." U.S. Patent Application No. 16/674,346.

Presentations and Tutorials

- "Run-time Accessible DRAM PUFs in Commodity Devices", at Top Picks in Hardware and Embedded Security, Westminster, CO, USA, Nov. 2019.
- Jakub Szefer, **Wenjie Xiong** and Shuwen Deng, "Secure Processor Architectures in the Era of Spectre and Meltdown", at IEEE International Symposium on Hardware Oriented Security and Trust (HOST), May 2019.
- "Dynamic PUFs and Software Protection", CASLAB Day, at Yale University, May 2019.
- "Run-time Accessible DRAM PUFs in Commodity Devices", at TU Darmstadt, Nov. 2016.
- "Run-time Accessible DRAM PUFs in Commodity Devices", at Conference on Cryptographic Hardware and Embedded Systems (CHES), Santa Barbara, CA, USA, Aug. 2016.

Teaching Experience

EENG 201 Introduction to Computer Engineering Teaching Assistant, Yale University *2017 Spring* and *2016 Spring*

- Topics include Boolean algebra, digital design, and basic computer architecture principles.
- Preparing lab materials, leading lab sessions, holding office hours, and grading.

Professional Service

Conference/Workshop Organizing

- Served as the Publications Chair for the IEEE International Symposium on Secure and Private Execution Environment Design (SEED 2021),
- Served as the Proceedings Chair for the 39th IEEE International Conference on Computer Design (ICCD) 2021,
- Served as the Publicity Chair for the 28th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2022).
- Served on the Organizing Committee of Secure and Private Systems for machine Learning (SPSL) workshop, co-located with ISCA 2021

Paper Review

Served on the Program Committees of the conferences/workshops:

- External PC of Architectural Support for Programming Languages and Operating Systems (ASPLOS 2022),

- the 39th IEEE International Conference on Computer Design (ICCD) 2021,
- External PC of Architectural Support for Programming Languages and Operating Systems (ASPLOS 2021),
- 9th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP 2020),
- 8th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP 2019),

Served as a reviewer for journals:

- ACM Computing Surveys (CSUR),
- IEEE Computer Architecture Letters (CAL),
- Design Automation for Embedded Systems (DAEM),
- IEEE Security & Privacy,
- IEEE Transactions on Circuits and Systems I,
- IEEE Transactions on Computers (TC),
- Advanced Electronic Materials,
- ACM Transactions on Architecture and Code Optimization (TACO),
- IEEE Design & Test,
- Nature Electronics,
- IEEE Access,
- International Journal of Circuit Theory and Applications (CTA),
- IEEE Consumer Electronics Magazine,
- ACM Transactions on Embedded Computing Systems (TECS),
- IEEE Transactions on Dependable and Secure Computing (TDSC).

Diversity and Inclusion Events

- Rising Stars in EECS 2020
- Career Workshop for Women and Minorities in Computer Architecture (CWWMCA) 2020
- Career Workshop for Women and Minorities in Computer Architecture (CWWMCA) 2019
- Improving the Diversity of Faculty in Electrical and Computer Engineering (iREDEFINE ECE) 2018
- Equity in the Job Search at Yale 2018
- Workshop for Women in Hardware and Systems Security (WISE) 2017
- CRA-W Grad Cohort 2016
- Workshop for women and underrepresented groups interested in computer security research (GREPSEC) II 2015